Journal of Military and Strategic Studies, Winter 2004, Vol. 7, Issue 3.

LA RÉVOLUTION DANS LES AFFAIRES TERRORISTES

Benoît Gagnon, Chaire Raoul-Dandurand en études stratégiques et diplomatiques, Université du Québec à Montréal (UQAM)

Introduction

Les attentats terroristes du 11 septembre 2001 ont profondément choqué les différentes populations du monde. En effet, ces attentats, d'une amplitude jusqu'alors jamais égalée, ont non seulement déstabilisé profondément la société américaine, mais ils ont aussi bouleversé fortement la psyché collective en engendrant un phénomène de peur généralisée.

Ce traumatisme de masse est dû au fait que les attentats du 11 septembre n'allaient pas dans la lignée des attentats terroristes traditionnels. « *Terrorists appear to be more imitative then innovative, although their tactics have changed in response to new defenses.*[1] » Ainsi, les attaques du 11 septembre avaient cela de différents : elles utilisaient des méthodes jusqu'alors inconnues pour la majorité des gens. Les tactiques étaient nouvelles et très spectaculaires. C'est cette différence, cette brisure avec la « routine » terroriste, qui a provoqué de tels remous dans les façons d'entrevoir le phénomène terroriste.

Ces événements ont fait naître beaucoup d'interrogations chez les spécialistes étudiant le terrorisme. Plusieurs se sont posés des questions sur les procédés à la base de l'organisation d'actes terroristes. Est-ce que le monde post-Guerre Froide caractérisé, entre autres, par la mondialisation et la montée des technologies de

l'information a engendré des transformations dans la manière d'employer les méthodes terroristes? Si oui, quelle est la nature exacte de cette mutation?

Au cours de ce texte, nous proposons d'étudier cette brisure avec le terrorisme traditionnel. Nous verrons en quoi le terrorisme a changé et vers quoi il se dirige. Ainsi, notre pensée se situe à mi-chemin entre celle de Paul Wilkinson[2] et de Walter Laqueur[3]. Si le premier croit profondément que les activités terroristes contemporaines tiennent plus du « *business as usual* », le second discute d'un terrorisme post-moderne, méconnaissable par rapport aux activités traditionnelles.

Sans pour autant prôner une argumentation démontrant que le terrorisme contemporain est fondamentalement différent, nous considérons que nous assistons présentement à une transformation dans la façon de structurer, de coordonner et de perpétrer les attentats terroristes. Ainsi, nous croyons que les associations terroristes façonnent de nouvelles techniques de combat qui, dans bien des cas, peuvent s'apparenter à la révolution dans les affaires militaires (RAM). De ce fait, nous serions en présence d'une révolution dans les affaires terroristes (RAT).

Notre argumentation se divise en quatre grandes étapes. Premièrement, nous définirons exactement ce que nous entendons par RAT. Cela nous permettra de mieux comprendre le phénomène en lui donnant un cadre conceptuel adéquat. Cette définition conceptuelle nous donnera aussi l'occasion de bien situer la RAT par rapport à la RAM.

---

[1] Brian M. Jenkins, « International Terrorism: The Other World War », dans Charles W. Kegley Jr. (ed.), *The New Global Terrorism: Characteristics, Causes, Controls*, Prentice Hall, Upper Saddle River, 2003, p. 24.

[2] Voir entre autres : Paul Wilkison, « Why Modern Terrorism? Differentiating Types and Distinguishing Ideological Motivations », dans Charles W. Keygley Jr., The New Global Terrorism: Characteristics, Causes, Controls, Prentice Hall, Upper Saddle River, 2003, p. 106-138.

[3] Walter Laqueur, « Postmodern Terrorism », *Foreign Affairs*, vol. 75, no. 5, septembre-octobre 1996, p. 24-36.

Deuxièmement, nous traiterons de la façon dont les organisations terroristes emploient les technologies de l'information pour améliorer l'efficacité de leurs opérations. Cette productivité accrue se fait à deux niveaux. Tout d'abord, elle permet d'amplifier les effets psychologiques de leurs actions. Ensuite, elle offre l'opportunité aux associations terroristes d'organiser leurs agissements plus efficacement, tout en leur donnant la possibilité de construire un modèle macro-organisationnel gérable.

Troisièmement, nous analyserons comment les structures terroristes contemporaines fonctionnent. Comme nous pourrons le voir, les possibilités offertes par les technologies de l'information aux terroristes leur permettent d'établir des structures hiérarchiques à la fois très complexes, très efficaces et plus résistantes aux opérations contre-terroristes. L'exemple d'Al-Qaida nous permettra d'illustrer ce point et de mieux faire comprendre au lecteur les transformations structurelles des hiérarchies terroristes.

Finalement, nous évaluerons comment la RAT transforme la définition de l'asymétrie. Il sera possible de constater que la RAT change non seulement la façon dont les groupes terroristes fonctionnent, mais elle laisse aussi émerger une nouvelle forme d'asymétrie; une asymétrie qui exploiterait à la fois les forces et les faiblesses de l'adversaire.

1. De la révolution dans les affaires militaires à la révolution dans les affaires terroristes

Durant les années 1990, les forces armées de différents États, mais surtout celles des États-Unis, ont modifié leurs structures organisationnelles afin de saisir le plein potentiel des technologies de l'information. Ce mouvement de réorganisation et d'intégration des technologies de l'information a été nommé la RAM.

Sans entrer dans les détails de ce qu'est une RAM, nous pouvons définir ce phénomène ainsi :

> Cette expression désigne une transformation radicale de la nature de la guerre, conséquence des percées technologiques qui, associées à des changements profonds de la doctrine militaire et des concepts organisationnels, modifient fondamentalement le caractère et la conduite des opérations militaires. Ces percées technologiques militaires ne constituent pas en soi une RAM; en effet, pour qu'il y ait « révolution », il faut que les nouvelles technologies conduisent à un changement profond de la doctrine et de l'organisation, ou qu'elles y trouvent leur répercussion.[4]

Dans le cadre de ce texte, il est intéressant de se pencher sur la RAM puisqu'elle se transpose aisément aux changements qui se sont produits au cœur des groupes terroristes depuis la fin de la Guerre Froide.

En effet, ce que l'on constate, c'est que les groupes terroristes ont enclenché des changements profonds dans leur façon d'opérer. Suite aux nombreux progrès sécuritaires attribuables soit à la RAM, soit aux technologies de l'information en général, les terroristes se sont retrouvés dans un contexte « stratégique » plus hostile. Conséquemment, ils ont dû user d'innovation pour faire face à cet environnement plus difficile et ont exploité certains principes émanant des innovations technico-organisationnelles en place afin de repenser leurs activités.[5]

---

[4] Elinor C. Sloan, « Le Canada et la révolution dans les affaires militaires: attitude actuelle et possibilités à venir », *Revue militaire canadienne*, vol. 1, no. 3, automne 2000, p. 7.

[5] Ce phénomène fait référence à ce que Colin S. Gray définit lui-même comme étant le défi nécessaire à la naissance d'une RAM. Selon lui, pour qu'une RAM puisse naître, il doit y avoir un défi stratégique à relever. C'est ce concours de circonstances stratégiques qui pousse les gens à innover et à conceptualiser des nouvelles façons d'employer les forces armées. Ce type de raisonnement peut donc s'appliquer aussi du côté des terroristes qui s'efforcent également à reconceptualiser leurs opérations dans des contextes sécuritaires changeant. Pour plus de détails, voir : Colin S. Gray, *Strategy for Chaos: Revolutions in Military Affairs and the Evidence of History*, Frank Cass, Portland, 2002.

En s'appropriant les innovations technologiques dans le domaine des communications et de l'informatique, les terroristes ont pu introduire des modifications importantes dans leurs activités, et ce, tant sur le plan organisationnel que sur le plan opérationnel. Nous serions donc en train d'assister à l'émergence d'une véritable révolution dans les affaires terroristes, qui allierait une mutation importante sur le plan structurel, juxtaposé à des méthodes originales d'utilisation des technologies de l'information.

Ainsi, en paraphrasant la définition de la RAM mentionnée précédemment, nous pourrions définir la RAT ainsi : elle désigne une transformation radicale de la nature des activités terroristes, conséquence des percées technologiques qui, associées a des changements profonds dans les objectifs des groupes terroristes et dans leur culture organisationnelle, modifient fondamentalement le caractère et la conduite des opérations terroristes.

Ces changements introduits par la RAT ont permis aux organisations terroristes de faire face, avec une efficacité grandissante, aux nouveaux défis apportés par la donne sécuritaire internationale contemporaine; un système à la fois plus poreux grâce à la mondialisation, et plus sécuritaire grâce aux outils technico-sécuritaires mis en place. Dans un premier temps, l'utilisation des technologies de l'information leur a permis d'accroître l'efficacité de leurs opérations. Dans un deuxième temps, ces mêmes technologies leur ont aussi apporté la possibilité de modifier leurs structures hiérarchiques, afin de pouvoir échapper aux autorités sécuritaires.

2. L'utilisation des technologies de l'information par les terroristes

Les technologies de l'information comme amplificateur de terreur

Dans le cadre opérationnel de l'utilisation des technologies de l'information, l'un des avantages le plus évident que l'intégration de ces technologies aura engendré pour ces groupes terroristes est de facilement manipuler l'information. Plus précisément, les technologies de l'information permettent aux terroristes d'employer indirectement à leur avantage la diffusion médiatique qui entoure leurs attentats. Dans ce cas, ces technologies agissent comme amplificateur de terreur.

Comme on le sait, le terrorisme a pour but d'inspirer la peur dans l'esprit des gens. Or, les médias jouent un rôle très important dans la propagation de la terreur.[6] En effet, en projetant et diffusant des images des actes terroristes et de leurs victimes, les médias aident les terroristes en leur donnant la publicité qu'ils recherchent.[7] En retransmettant des images chocs sur plusieurs chaînes médiatiques, les journalistes martèlent l'esprit des citoyens avec des symboles inspirant la crainte. Or, avec la montée rapide des technologies de l'information, ce mouvement s'est promptement décuplé. Les journalistes sont désormais capables d'envoyer instantanément leurs clichés partout dans le monde, ce qui permet aux gens de vivre en direct le traumatisme terroriste.

À cela s'ajoute le fait que les journalistes ne sont désormais plus en position de « monopole de l'information », au sens où l'Internet démocratise à grande échelle la diffusion d'images et de contenu. La facilité de créer un site Web et de mettre des

[6] À ce sujet, voir : Pippa Norris, Montague Kern et Marion Just (ed.), *Framing Terrorism: The News Media, the Government, and the Public*, Routledge, New York, 2003, 329 p.

informations en ligne change fortement l'influence que peut avoir un individu ou un petit groupe d'individus sur la circulation d'images évoquant la terreur.

L'exemple le plus frappant de cela est assurément l'affaire Daniel Pearl. Ce journaliste américain, enlevé le 23 janvier 2002 à Karachi, au Pakistan, par un groupe se faisant appeler le *Mouvement National pour la Restauration du Pakistan*, s'est fait décapité par ses ravisseurs le 29 ou le 30 janvier 2004. Or, non seulement les ravisseurs ont employé Internet pour envoyer leurs exigences au gouvernement américain[8], mais la vidéo montrant la décapitation de Daniel Pearl s'est rapidement retrouvée sur Internet et a provoqué une vague d'indignation mondiale.

Les terroristes ont donc utilisé des outils relativement simples - des ordinateurs et leurs applications - pour se faire de la publicité. Contrairement aux méthodes traditionnelles de propagande, les terroristes n'ont pas eu besoin d'attendre les journalistes pour présenter leurs méfaits aux yeux du monde. En utilisant la dissémination électronique des images de l'exécution de Daniel Pearl, les terroristes ont pu créer un effet psychologique avant même que leurs actions violentes soient reprises par les médias. Ces derniers n'ont fait que reprendre cette commotion et l'ont amplifié. Cela démontre donc avec force comment les technologies numériques servent comme amplificateur de la terreur.[9]

---

[7] Comme le note Cindy C. Combs, il importe peu aux groupes terroristes que cette publicité soit négative ou positive. Ce qu'ils recherchent avant tout est de sortir de l'ombre et pouvoir se faire connaître et faire connaître leurs revendications au public. Voir Cindy C. Combs, *Terrorism in the Twenty-First Century*, Prentice Hall, Upper Saddle River, 2003.

[8] Les terroristes avaient utilisé le service de courriel Hotmail offert par Microsoft et ont ouvert un compte portant le nom kidnapperguy@hotmail.com. Ce compte a été l'hôte des conversations entre les ravisseurs et le gouvernement américain.

[9] Voir, entre autres, Wordiq.com, *Daniel Pearl*, (page consutée le 1 septembre 2004), [en ligne], adresse URL : http://www.wordiq.com/definition/Daniel_Pearl

Plus près de nous encore, nous pouvons mentionner l'affaire Nick Berg. En diffusant les images de la décapitation de Nick Berg sur un site Web, les terroristes membres du réseau d'Abou Mussab Al-Zarqaoui ont su utiliser le potentiel réseautique et multiplicateur de l'Internet. En très peu de temps, les images de l'exécution de Nick Berg ont fait le tour du monde.[10] Ces dernières ont été reprises par les médias et ont conséquemment instauré un sentiment de peur dans l'esprit des gens.

Comme on peut le constater, les terroristes peuvent désormais être les diffuseurs principaux de leur propre campagne de terreur. En plaçant sur l'Internet des images inspirant la terreur, ils utilisent les technologies de l'information comme amplificateur de celle-ci.

Les groupes terroristes et la cyberplanification

Un autre outil important fourni par les technologies de l'information aux groupes terroristes est la cyberplanification. La cyberplanification consiste à utiliser les technologies de l'information - majoritairement l'Internet, mais aussi les téléphones cellulaires, les messageries textes instantanées, etc. - pour gérer les activités d'un groupe. Dans le cadre des organisations terroristes, la cyberplanification leur fournit cinq avantages :

1. Elle aide différents membres d'un ou plusieurs réseaux terroristes à communiquer entre eux. Les sites Internet servent alors de portails de

[10] Le fichier a été téléchargé des dizaines de milliers de fois, replacé sur d'autres sites Internet et est demeuré en tête de liste sur les moteurs de recherche pendant des jours.

discussions ou permettent d'échanger des informations[11] de manière secrète[12] via l'utilisation de la stéganographie[13] et de la cryptologie[14].

2. Elle permet d'obtenir un financement par le biais de donations ou via l'exploitation de différents sites Internet corporatifs.[15]
3. Elle offre un commandement et un contrôle très efficace des opérations.

> *Command and control on the Internet is not hindered by geographical distance, or by lack of sophisticated communications equipment.* […] *Terrorists can use their front organizations to coordinate such attacks, to flood a key institution's e-mail service (sometimes as a diversionary tactic for another attack), or to send hidden messages that coordinate and plan future operations.*[16]

L'Internet, et les technologies de l'information en général, permettent donc de coordonner aisément les activités d'une organisation terroriste, et ce, de manière quasi anonyme.

4. Un autre grand avantage est la facilité de recrutement. Autrefois, un groupe terroriste qui voulait se faire connaître et attirer des membres à grande échelle devait faire des coups d'éclats et susciter l'attention des médias. Aujourd'hui, avec l'Internet, un groupe terroriste n'a pas besoin de faire d'attentats pour toucher une audience mondiale; il n'a qu'à y avoir un site Web et le monde a

---

[11] À ce titre, le site Internet http://www.jihadunspun.net est fortement suspecté par les autorités américaines de fournir aux terroristes islamistes un lieu d'échange rapide et efficace. Au moment de la rédaction de cet article, ce site abritait d'ailleurs un message d'Oussama ben Laden d'environ 13 minutes.

[12] Notons par exemple le site https://www.spammimic.com/ qui permet de crypter un message pour le faire passer pour du pourriel. Une personne qui intercepterait un message crypté aurait donc l'impression qu'il s'agit simplement d'un courriel publicitaire.

[13] La stéganographie consiste à dissimuler un document électronique dans un autre, par exemple, un texte dans une image. Cela complique donc grandement l'interception des fichiers qui ne sont pas légitimes. Surtout si le document caché est encrypté.

[14] La cryptologie consiste à encoder un message par des algorithmes, le rendant ainsi indéchiffrables sans avoir la clef de déchiffrement.

[15] On sait entre autres qu'une partie des activités terroristes se finance via l'exploitation de sites Web de pornographie infantile. À ce sujet, voir : Jacky Rowland, *Russia is 'major child porn source'*, (page consultée le 26 avril 2004), [en ligne], adresse URL : http://news.bbc.co.uk/1/hi/world/europe/2543717.stm

instantanément accès à ses idées. L'Internet représente un instrument marketing très efficace :

> *Individuals with sympathy for a cause can be converted by the images and messages of terrorist organizations, and the addition of digital video has reinforced this ability. Images and video clips are tools of empowerment for terrorists. More important, net access to such products provides contact points for men and women to enroll in the cause, whatever it may be.*[17] »

Cette efficacité se voit d'autant plus importante du fait qu'elle emploie très peu de ressources. Le calcul coûts versus bénéfices est ainsi très positif pour ces organisations.

D'ailleurs les réseaux terroristes utilisent actuellement le recrutement sur Internet. Jessica Stern soulève entre autres que :

> […] *according to U.S. government officials, al Qaeda now uses chat rooms to recruit Latino Muslims with U.S. passports, in the belief that they will arouse less suspicion as operatives than would Arab-Americans.*[18]

Cet exemple représente très bien comment l'Internet est un outil de recrutement efficace en leur permettant d'atteindre d'éventuels adhérents partout dans le monde.

5. Finalement, l'Internet offre aux terroristes l'avantage indéniable d'être une source très importante d'informations sur des cibles potentielles. Quand on sait que plus de 80% des données utilisées par les différentes agences de la communauté du

---

[16] Timothy L. Thomas, « Al Qaeda and the Internet: The Danger of "Cyberplanning" », *Parameters*, vol. 33, no. 1, printemps 2003, p. 117.
[17] *Ibid*., p. 118.
[18] Jessica Stern, « The Protean Enemy », *Foreign Affairs*, vol. 82, no. 4, juillet-août 2003, p. 35.

> renseignement proviennent dorénavant de sources ouvertes[19], il est légitime de croire que les organisations terroristes peuvent fonctionner de la même façon. En employant des informations disponibles sur l'Internet, les terroristes découvrent les cibles à risque et peuvent choisir celles qui sont les plus intéressantes pour eux.

Un des meilleurs exemples de cyberplanification que nous pouvons citer est celui s'étant produit à la veille des attentats de Madrid perpétrés par la nébuleuse d'Al-Qaida en avril 2004. En effet, non seulement l'attentat a été planifié sur le Web, - plus spécifiquement sur des forums de discussions - mais les conséquences de l'attentat, soit le retrait des troupes espagnoles de l'Irak, avaient également été prévues par les organisateurs de l'attaque. [20]

Ainsi, en employant des méthodes de communication très modernes, Al-Qaida a réussi a fomenter un attentat, et ce, sans organiser de réunion physique entre ses membres. En fait, ce que l'on constate par rapport aux activités informatiques du groupe terroriste, c'est que depuis l'invasion en Afghanistan, Al-Qaida s'est presque complètement tourné vers le Web pour s'organiser. « *Al-Qaeda is moving between 50 different Web addresses and has set up what they call online training camps* […][21] » Ce type d'E-organisation a l'avantage d'éviter les nombreux déplacements des membres du groupe, leur donnant ainsi plus de chance d'éviter de se faire détecter par les

---

[19] Bruce D. Berkowitz et Allan E. Goodman, *Best Thruth : Intelligence in the Information Age*, Yale University Press, Londres, 2000, p. 78 (traduction libre).

[20] À ce sujet, voir : Douglas Frantz, Josh Meyer et Richard B. Schmitt, *Cyberspace Gives Al Qaeda Refuge*, (page consultée le 31 août 2004), [en ligne], adresse URL : http://news.yahoo.com/news?tmpl=story&u=/latimests/20040815/ts_latimes/cyberspacegivesalqaedarefuge

[21] Kevin Anderson, *Militants weave web of terror*, (page consultée le 3 septembre 2004), [en ligne], adresse URL : http://news.bbc.co.uk/2/hi/technology/3889841.stm

autorités sécuritaires. De même, quand on considère que l'Internet est un « espace » relativement anonyme, il devient d'autant plus facile d'établir des communications efficaces entre différentes cellules terroristes.

Par ailleurs, cette tendance vers la cyberplanification se voit dans le nombre de sites Internet appartenant à des groupes terroristes et qui apparaissent sur la toile, comme cela est possible de le voir dans cette typologie.[22]

- Hamas :
    - http://www.hamas.org (1998)
    - http://www.palestine-info.net/hamas.index.htm (1998)
    - http://www.palestine-info.com/index_e.htm (2002)
    - http://www.qassam.org (2002)
- Hezbollah :
    - http://www.hizbollah.org (1998, 2002)
    - http://www.moqawama.org (1998)
    - http://www.moqawama.tv (2002)
    - http://wwwalmanar.com.lb (2002)
- PKK : http://www.pkk.org (1998 et 2002)
- FPLP : http://www.pflp-pal.org/about.html
- Mouvement islamique de l'Ouzbékistan : http://www.ummah.net/uzbekistan

Le fait que ces groupes terroristes ayant une idéologie islamique radicale aient décidé d'utiliser à fond l'Internet pour communiquer, démontre l'ampleur que prend le phénomène de la cyberplanification.

---

[22] Voir : Yariv Tsfati et Gabriel Weimann, « www.terrorism.com: Terror on the Internet », *Studies in Conflict and Terrorism*, vol. 25, no. 5, 2002, p. 317-332.

3. La « Réseautisation » des activités terroristes

Une des difficultés à laquelle les autorités politiques devront faire face en ce qui a trait aux groupes terroristes c'est leurs changements sur le plan organisationnel. La tendance la plus marquante que nous pouvons identifier par rapport aux organisations terroristes est que leurs structures organisationnelles s'agencent selon les théories issues de la loi de Metcalfe. La loi de Metcalfe stipule que la force – ou la valeur - d'un réseau est proportionnelle au carré du nombre de ceux qui l'utilisent.[23]

Au niveau social, cela signifie que si des gens interagissent ensemble vers un objectif commun, ils décupleront leurs capacités d'action. Par exemple, trois terroristes collaborant de manière isolée peuvent être nuisibles, mais ils le sont beaucoup moins que s'ils travaillent ensemble. De là l'application de la loi de Metcalfe dans la théorisation des organisations terroristes.

Les études effectuées par David Rondfelt et John Arquilla[24] semblent confirmer cette tendance à la « réseautisation » des structures organisationnelles terroristes. En fait, selon leurs travaux, les groupes terroristes se tourneraient de plus en plus vers quatre types de structures réseautiques. Ces quatre formes d'organisations ont des variantes importantes. En effet, comme nous le verrons plus bas, chacune d'entre elles comporte des avantages et des inconvénients. Tout dépendant du modèle adopté, les nœuds des réseaux varient selon leurs fonctions et leur importance stratégique.[25]

---

[23] Charles Boyd, *Metcalfe's Law*, (page consultée le 3 août 2004), [en ligne], adresse URL : http://www.mgt.smsu.edu/mgt487/mgtissue/newstrat/metcalfe.htm.

[24] John Arquilla et David Rondfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, National Defense Institute RAND, Santa Monica, 2001.

[25] Une typologie similaire traitant des nœuds réseautique des groupes terroristes a été faite par Jacques Baud : Voir Jacques Baud, *La guerre asymétrique ou la défaite du vainqueur*, Du Rocher, Paris, 2003, p. 55. Nous nous dissocions toutefois de l'analyse qui en est faite. En effet, Baud traite des nœuds critiques et névralgiques sous une vision clausewitzienne, en les comparant au concept de « centre de gravité », ce qui implique que ces nœuds seraient en fait les points faibles des organisations. Sans rejeter complètement cette vision, nous n'adhérons pas complètement à cette analyse. Le concept de

Les noeuds critiques sont ceux qui représentent le haut de la hiérarchie décisionnelle. Sans être indispensables au fonctionnement de l'organisation, ils représentent tout de même la base stratégique des groupes terroristes; c'est à cet endroit que les décisions les plus importantes sont prises sur les actions en cours et à venir.

Les nœuds névralgiques, de leur côté, constituent les membres qui dépendent en partie des « chefs », - surtout au niveau idéologique - mais pouvant très bien diriger la majorité des activités du groupe, et ce, de manière autonome. Ils représentent habituellement les cadres intermédiaires des organisations terroristes. Ce sont souvent eux qui s'occupent majoritairement de la formation, du recrutement et de la gestion « au quotidien » de l'organisation terroriste.

Pour leur part, les noeuds opérationnels représentent les « soldats » des organisations terroristes. Ce sont eux qui fomentent les activités du groupe, en planifiant les tactiques à employer pour commettre leurs attentats. Bref, ce sont eux qui sont à l'avant plan. Malgré tout, ils partagent des tâches avec les cadres intermédiaires en touchant à l'acquisition de l'armement, au financement, au recrutement, etc. Toutefois, ce degré de contrôle varie selon la structure adoptée et aussi en fonction de chaque groupe terroriste.[26] Voyons donc quelles sont les quatre formes de hiérarchies réseautiques qui sont à la disposition des groupes terroristes.

Clausewitz a été formulé en fonction d'une vision militaire classique où la structure organisationnelle est régie par une hiérarchie militaire rigide et structurée. Or, il est de notre avis que les organisations terroristes se distinctes justement des armées de par le fait qu'elles emploient des structures organisationnelles souples, polyvalentes et capables de subir des assauts dans leur soi-disant « centre de gravité » tout en maintenant leurs opérations.

[26] Par exemple, l'IRA délègue moins de responsabilités aux membres inférieurs de l'organisation que ce que l'on peut voir avec Al-Qaida.

Les quatre structures réseautiques

Le réseau en chaîne

Le réseau en chaîne est un réseau qui s'apparente à la hiérarchie pyramidale classique. Il s'agit d'une structure linéaire où les deux extrémités – les têtes de l'organisation d'un côté et les exécutants de l'autre - sont séparées par des nœuds réseautiques, c'est-à-dire des composantes organisationnelles, servant à disséminer l'information et à délester la tête du réseau de certaines responsabilités.

Si cette structure est efficace, car elle implique que les ordres vont directement en bas de l'échelle, elle est toutefois fragile face aux autorités sécuritaires. En effet, si la tête est mise hors circuit, toute l'organisation risque de tomber. De même, si un des niveaux inférieurs est enlevé, l'organisation perd de sa cohérence rapidement.

Le réseau en étoile

Le réseau en étoile est une version plus décentralisée du réseau en chaîne. Il n'utilise pas (ou peu) de nœuds névralgiques; les ordres vont donc directement des têtes dirigeantes vers les nœuds opérationnels. Ces derniers sont en charge de coordonner leurs activités et se doivent de faire le gros du travail qui est normalement entre les mains des cadres intermédiaires. Ce type de réseau est très efficace, il permet d'avoir plusieurs petits groupes chargés des opérations qui sont dirigés en même temps, mais comme le réseau en chaîne, il est également très fragile face aux opérations policières.

Le réseau franchisé

Le réseau franchiséimplique plusieurs nœuds réseautiques interconnectés entre eux, ainsi qu'à un nœud central coordonnant les activités. « *The strength of this form of organization is that all cells are independent of one another and the discovery of one cannot lead to the discovery of another.*[27] » En effet, advenant la chute du noeud critique, qui consiste surtout en un phare idéologique pour le groupe, les cadres intermédiaires peuvent tout de même reprendre le relais et poursuivre les opérations terroristes.

Notons qu'aujourd'hui plusieurs groupes terroristes s'organisent selon ce type de structure. Cet archétype organisationnel permet un fonctionnement possédant à la fois, la souplesse d'un réseau décentralisé, et l'efficacité d'un réseau hiérarchisé où le pouvoir décisionnel est bien informé et capable de faire circuler l'information rapidement. Néanmoins, il faut admettre que ce type de structure laisse de plus en plus de place au réseau à matrice complexe.

Le réseau à matrice complexe : la conséquence directe de la RAT sur les structures terroristes

Le dernier type de réseau est le réseau à matrice complexe ou à canaux multiples. Cette structure a pour caractéristique de relier tous les nœuds pris individuellement avec tous les autres nœuds, créant ainsi un filet d'interconnexions. Le principal avantage de ce type de forme organisationnelle est qu'il crée un environnement décisionnel « sans tête » (*leaderless*).

Cette structure sans tête offre de nombreux avantages. Le premier fait référence à la notion de « réseau-stupide » Ce concept, issu des travaux de David Isenberg sur les réseaux téléphoniques[28], énonce que lorsqu'il doit opérer dans un contexte d'incertitude – comme dans le cadre de l'organisation d'un réseau terroriste par exemple – un réseau ne devrait jamais être optimisé en fonction de l'élaboration d'une action particulière. Un réseau agissant dans un contexte d'incertitude devrait plutôt adopter le fonctionnement le plus simple afin d'assurer son efficacité dans le plus grand nombre de situations possibles. En évitant de surspécialiser les différentes composantes de l'organisation dans une tâche bien définie, un réseau devient donc plus polyvalent.

Ainsi, les différentes composantes du réseau doivent être assez habiles pour pouvoir sortir de leurs fonctions de départ. C'est-à-dire que les cellules d'un réseau doivent être aptes à se mouler aux diverses situations qui peuvent se produire et ce, même si ce n'était pas dans les responsabilités qui leur avaient été dévolues au départ. L'adoption d'une structure en réseau à matrice complexe permet donc à l'organisation de pouvoir s'acquitter de tâches très diverses; allant de l'attentat terroriste jusqu'aux opérations de financement par le commerce de la drogue.

Autre avantage : ce type de structure offre aux terroristes la latitude de faire travailler la fourmilière, plutôt que d'engager la reine dans des tâches plus terre-à-terre. En d'autres mots, la structure en réseau à matrice complexe tend à s'auto-organiser de manière quasi biologique, axant subséquemment le travail des chefs-terroristes vers la direction générale du groupe, plutôt que vers la gestion au quotidien des activités.

---

[27] Brad McAllister, « Al Qaeda and the Innovative Firm: Demythologizing the Network », *Studies in Conflict and Terrorism*, vol. 27, no. 4, juillet 2004, p. 302.

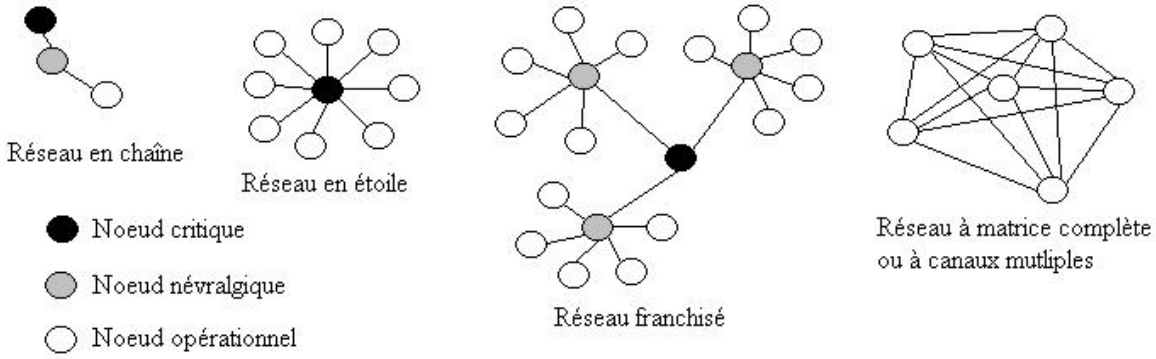
[28] Voir : David Isenberg, *Rise of the Stupid Network*, (page consultée le 20 octobre 2004), [en ligne], adresse URL : http://www.rageboy.com/stupidnet.html

Or, non seulement cela rend les hauts-responsables moins présents dans la gestion quotidienne des activités du groupe, mais cela leur permet également de bénéficier d'un écart par rapport aux actions du groupe. Les autorités terroristes ne sont donc jamais vraiment responsables des actions du réseau. Les chefs ne prennent pas de décisions directes; ils suggèrent plutôt que certaines actions seraient plus utiles que d'autres. Ce type de direction complique grandement les activités des autorités sécuritaires qui doivent donc décoder les suggestions des gestionnaires terroristes.

Il est clair que cette structure organisationnelle est de plus en plus populaire chez les groupes terroristes, car non seulement elle est efficace, mais elle permet aussi au réseau de faire diminuer grandement son niveau de vulnérabilité. « *Having no "hub" to answer to, authority in an all-channel network is entirely decentralized, minimalizing the impact of the destruction of individual cells on the organization as a whole.*[29] » Étant donné que chacune des cellules de l'organisation n'est pas surspécialisée et demeure polyvalente, elle peut continuer son travail de manière indépendante, et ce, même si d'autres cellules appartenant à l'organisation se voient démantelées.

En fait, le seul désavantage majeur avec ce type de configuration hiérarchique est son frein à l'innovation. En effet, étant donné que les « cerveaux » ont moins d'influence sur la structure et qu'ils prennent moins de place dans l'organisation, ils peuvent plus difficilement apporter des idées innovatrices à leurs membres. Il est donc à prévoir que les groupes terroristes qui emprunteront cette forme organisationnelle risquent d'avoir de la difficulté à faire des attentats très novateurs.

En définitive, il est également important de noter que ce type d'organisation est la résultante directe de l'utilisation des technologies de l'information. En effet, sans les systèmes de communication (Internet, réseaux cellulaires, etc.) que nous offrent les technologies actuelles, il serait quasi impossible de bien gérer une organisation dont la structure serait construite en matrice complexe. Cette structure est donc la conséquence directe d'une modification structurelle permettant d'exploiter au maximum les technologies de l'information.



Les changements de structures : l'exemple d'Al-Qaida

Ce qui est intéressant de souligner, c'est que la structure en réseau à matrice complexe est relativement récente chez les organisations terroristes. En fait, c'est un défi stratégique qui a poussé les autorités terroristes à modifier leurs configurations organisationnelles. L'exemple de plus probant de cette situation se retrouve dans le réseau terroriste Al-Qaida. Avant l'opération américaine en Afghanistan, l'organisation

[29] Brad McAllister, *loc. cit.*, p. 302.

adoptait la structure franchisée. C'est ce qui lui a permis d'être aussi efficace et de mettre sur pied une opération si bien coordonnée que celle du 11 septembre.

Toutefois, depuis que les États-Unis ont ébranlé le réseau terroriste dans son sanctuaire afghan, la situation s'est drastiquement modifiée. « *While al Qaeda clearly continues to benefit from certain strengths, it must now operate in a less-permissive environment.*[30] » Ainsi, pour pouvoir poursuivre ses opérations dans un environnement plus difficile pour lui, Al-Qaida a dû s'adapter et adopter un nouveau mode de fonctionnement.

> Aujourd'hui, Al Qaida connaît une période de transition. […] Malgré le démantèlement de son infrastructure opérationnelle et de formation en Afghanistan, Al Qaida s'adapte en cherchant à établir ses bases ailleurs et, de ce fait, demeure une menace sérieuse, immédiate et directe pour ses ennemis. Bien que partout dans le monde, l'infrastructure matérielle et humaine d'Al Qaida ait souffert, son réseau à travers le monde, constitué de multiples strates, a conservé une profondeur suffisante pour planifier, préparer et exécuter des opérations, soit directement, soit par le truchement des groupes qui lui sont associés.[31]

En d'autres termes, la structure réseautique franchisée prônée par Al-Qaida a été changée pour une structure réseautique à matrice complexe.

Pour faire face à un contexte sécuritaire plus difficile pour elle, l'organisation a dû emprunter une structure qui lui permettait de protéger ses acquis et de se mouvoir aisément à travers les mailles des forces policières. La structure réseautique à matrice complexe répond entièrement à ce besoin. En n'ayant pas de hiérarchie spécifique, en d'autres mots en ne possédant pas de nœud réseautique dirigeant les autres, Al-Qaida a pu continuer à mener la plupart de ses activités.

---

[30] Brian M. Jenkins, *Countering al Qaeda: An Appreciation of the Situation and Suggestions for Strategy*, National Defense Institute RAND, Santa Monica, 2002, p. 10.

[31] Rohan Gunaratna, « Le nouveau visage d'Al Qaida : La menace du terrorisme islamiste après le 11 septembre », dans Gérard Chaliand et Arnaud Blin (dir.), *Histoire du terrorisme : de l'Antiquité à Al Qaida*, Bayard, Parirs, 2004, p. 465.

De même, cette structure a permis d'intégrer aisément toute une panoplie d'autres organisations qui gravitaient autour d'Al-Qaida sans en faire vraiment partie. La structure « sans chef » répartit l'autorité décisionnelle dans tous les nœuds de la structure, ce qui permet un recrutement plus efficace et plus diffusé.[32] C'est entre autres pour cette raison qu'Al-Qaida s'est grandement complexifiée et qu'il est désormais commun de parler de la nébuleuse d'Al-Qaida.

C'est aussi parce qu'Al-Qaida a employé cette configuration hiérarchique depuis les attentats du septembre 2001, qu'elle sombre dans une incapacité à innover. Comme nous l'avons précédemment mentionné, le réseau à matrice complexe tend à distancer les chefs porteurs des idées novatrices, des militants. Or, selon toute vraisemblance, c'est ce qui se produit actuellement dans la nébuleuse d'Al-Qaida. Certes, le groupe est plus efficace et plus actif, mais, pour l'instant du moins, il demeure cloisonné dans deux formes d'attentats : les explosions et les enlèvements.

4. Une nouvelle façon d'employer les méthodes asymétriques

Au-delà des transformations sur le plan opérationnel et sur le plan organisationnel, ce qui est intéressant de constater avec cette RAT, c'est qu'elle modifie profondément la façon dont les groupes terroristes peuvent employer l'asymétrie. De manière traditionnelle, nous pouvons définir l'asymétrie de deux façons : l'asymétrie négative et l'asymétrie positive.[33]

[32] À ce titre, une récente études faite par le International *Institute for Strategic Studies* démontre qu'Al-Qaida a des cellules actives dans environ 60 pays. Voir : Richard Norton-Taylor, *Thinktank: invasion aided al-Qaida*, (page consultée le 20 octobre 2004), [en ligne], adresse URL : http://www.guardian.co.uk/Iraq/Story/0,2763,1331362,00.html

L'asymétrie correspond à une méthode utilisée par un acteur incapable d'affronter de manière conventionnelle un adversaire trop fort pour lui. Du côté de l'asymétrie négative, cette technique de combat passe par l'exploitation des faiblesses de l'adversaire. En d'autres termes, cela consiste donc à frapper le « ventre mou » (*underbelly*) de l'ennemi plutôt que de s'acharner sur des endroits mieux protégés.

L'asymétrie positive, de son côté, propose un raisonnement inverse. Il ne s'agit pas d'exploiter les faiblesses de l'adversaire, mais plutôt d'employer ses forces. Ainsi, un peu à l'image des techniques d'Aïkido, il faut utiliser judicieusement les forces de l'adversaire pour les rediriger contre lui-même.[34]

Or, ce qu'il y a de nouveau avec le terrorisme contemporain, c'est qu'il met en place une nouvelle forme d'asymétrie; une asymétrie positive-négative. Elle est positive, car elle utilise adroitement les forces de l'ennemi, dans ce cas-ci le potentiel offert par les technologies de l'information. En même temps, cette asymétrie est négative, car elle reprend ces forces pour les utiliser contre les points faibles de nos sociétés. Cela renforce donc d'autant plus la position du faible par rapport au fort, ce dernier se trouvant dans une position plus précaire voyant ses forces et ses faiblesses utilisées contre lui.

Conclusion

Comme il nous a été possible de le voir, nous sommes présentement en train de vivre une transformation majeure dans les affaires terroristes. La façon dont les

---

[33] Pour une définition très complète de ce qu'est l'asymétrie, voir : Jacques Baud, *La guerre asymétrique ou la défaite du vainqueur*, Du Rocher, Paris, 2003.

[34] Cette analogie a d'ailleurs été employée par Thomas Homer-Dixon dans son article paru dans le *Foreign Policy* suivant les événements du 11 septembre et qui discutait de la montée de ce qu'il définit comme étant du terrorisme complexe. Voir : Thomas Homer-Dixon, « The Rise of Complex Terrorism », *Foreign Policy*, janvier-février 2002, p. 52 à 62.

organisations terroristes ont employé les technologies de l'information, et les changements organisationnels qui en résultent, nous prouvent que nous voyons se produire une révolution dans les affaires terroristes.

Ces importantes transformations se dénotent, entre autres, à travers l'utilisation que les terroristes font des technologies de l'information pour accentuer la peur résultant de leurs attentats. En employant le potentiel communicationnel déployé par les nouvelles technologies, les organisations terroristes réussissent à véhiculer leurs revendications et à publiciser leurs actes, et ce, en ne dépendant plus des médias pour le faire.

Néanmoins, c'est surtout au chapitre de la cyberplanification et sur le plan de la réorganisation structurelle que la RAT se fait le plus sentir. Non seulement l'exploitation des nouvelles technologies permet aux groupes terroristes d'être plus efficaces pendant leurs opérations, mais cela leur donne aussi l'occasion de structurer leur hiérarchie de façon à la rendre plus apte à répondre à un contexte sécuritaire plus hostile à leurs activités.

En somme, si l'histoire militaire tend à démontrer que les RAM deviennent désuètes quand plusieurs autres États se dotent de moyens similaires ou permettant de contrecarrer ces avancés technico-militaires, le XXIe siècle est bien différent. Ce qui est important de mentionner, c'est que cette RAT se trouve, en fait, être une forme de réponse aux transformations échafaudées par les autorités sécuritaires via la RAM. Elle permet d'exploiter les faiblesses inhérentes aux sociétés, mais surtout de limiter les effets positifs de la RAM en utilisant les technologies qui la sous-tendent pour la rendre moins efficace. Un exemple probant de cette situation est l'utilisation de la cryptographie et de la stéganographie par les groupes terroristes; même si les autorités sécuritaires

bénéficient des technologies poussées pour détecter les activités terroristes, cette même technologie permet à ces organisations illicites de mieux cacher leurs opérations.

Ainsi, nous pourrions dire que ce phénomène constitue, en quelque sorte, une contre-révolution dans les affaires militaires (CRAM). Toutefois, contrairement à ce que l'histoire nous a habitué à voir, cette CRAM n'est pas possédée par un pouvoir politique social au sens plus classique du terme. Pour la première fois, elle se trouve entre les mains d'organisations qui ne répondent pas à un pouvoir politique centralisé, mais bien à des intérêts détenus par de petits groupes d'individus.

Bibliographie

Anderson, Kevin, *Militants weave web of terror*, (page consultée le 3 septembre 2004), [en ligne], adresse URL : http://news.bbc.co.uk/2/hi/technology/3889841.stm

Arquilla, John et David Rondfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, National Defense Institute RAND, Santa Monica, 2001.

Baud, Jacques, *La guerre asymétrique ou la défaite du vainqueur*, Du Rocher, Paris, 2003.

Berkowitz, Bruce D. et Allan E. Goodman, *Best Thruth : Intelligence in the Information Age*, Yale University Press, Londres, 2000.

Boyd, Charles, *Metcalfe's Law*, (page consultée le 3 août 2004), [en ligne], adresse URL : http://www.mgt.smsu.edu/mgt487/mgtissue/newstrat/metcalfe.htm

Chaliand, Gérard et Arnaud Blin (dir.), *Histoire du terrorisme : de l'Antiquité à Al Qaida*, Bayard, Parirs, 2004.

Combs, Cindy C., *Terrorism in the Twenty-First Century*, Prentice Hall, Upper Saddle River, 2003.

Frantz, Douglas, Josh Meyer et Richard B. Schmitt, *Cyberspace Gives Al Qaeda Refuge*, (page consultée le 31 août 2004), [en ligne], adresse URL : http://news.yahoo.com/news?tmpl=story&u=/latimests/20040815/ts_latimes/cyberspacegivesalqaedarefuge

Gray, Colin S., *Strategy for Chaos: Revolutions in Military Affairs and the Evidence of History*, Frank Cass, Portland, 2002.

Homer-Dixon, Thomas, « The Rise of Complex Terrorism », *Foreign Policy*, janvier-février 2002, p. 52 à 62.

Isenberg, David, *Rise of the Stupid Network*, (page consultée le 20 octobre 2004), [en ligne], adresse URL : http://www.rageboy.com/stupidnet.html

Jenkins, Brian M., *Countering al Qaeda: An Appreciation of the Situation and Suggestions for Strategy*, National Defense Institute RAND, Santa Monica, 2002.

Kegley, Charles W. Jr. (ed.), *The New Global Terrorism: Characteristics, Causes, Controls*, Prentice Hall, Upper Saddle River, 2003.

Laqueur, Walter, « Postmodern Terrorism », *Foreign Affairs*, vol. 75, no. 5, septembre-octobre 1996, p. 24-36.

McAllister, Brad, « Al Qaeda and the Innovative Firm: Demythologizing the Network », *Studies in Conflict and Terrorism*, vol. 27, no. 4, juillet 2004, p. 297-319.

Norris, Pippa, Montague Kern et Marion Just (ed.), *Framing Terrorism: The News Media, the Government, and the Public*, Routledge, New York, 2003.

Norton-Taylor, Richard, *Thinktank: invasion aided al-Qaida*, (page consultée le 20 octobre 2004), [en ligne], adresse URL : http://www.guardian.co.uk/Iraq/Story/0,2763,1331362,00.html

Rowland, Jacky, *Russia is 'major child porn source'*, (page consultée le 26 avril 2004), [en ligne], adresse URL : http://news.bbc.co.uk/1/hi/world/europe/2543717.stm

Sloan, Elinor C., « Le Canada et la révolution dans les affaires militaires: attitude actuelle et possibilités à venir », *Revue militaire canadienne*, vol. 1, no. 3, automne 2000, p. 7-14.

Stern, Jessica, « The Protean Enemy », *Foreign Affairs*, vol. 82, no. 4, juillet-août 2003, p. 27-40.

Thomas, Timothy L., « Al Qaeda and the Internet: The Danger of “Cyberplanning” », *Parameters*, vol. 33, no. 1, printemps 2003, p. 112-123

Tsfati, Yariv et Gabriel Weimann, « www.terrorism.com: Terror on the Internet », *Studies in Conflict and Terrorism*, vol. 25, no. 5, 2002, p. 317-332.

Wordiq.com, *Daniel Pearl*, (page consutée le 1 septembre 2004), [en ligne], adresse URL : http://www.wordiq.com/definition/Daniel_Pearl